REMARKS

Claims 1-3, 6, 8, 9, 14, 17 and 21-23 are amended to more clearly define the invention.

Support for the amendments is found in the existing claims and in the Application description in connection with Figure 2 and other places. Specifically, support for "automatically communicating application specific context information to a particular application of said plurality of different applications in response to a user command to initiate execution of said particular application and in response to automatic logon to said particular application via said single logon menu" is found in the Application on page 5 lines 25-37 and lines 31-33. This section indicates "Manager 250 employs a system protocol for passing session context information to applications 200 and 230 via URL query or form data. The session context information comprises a session identifier, a hash value, and application specific data. ... The application specific data is tailored to meet the intended function of a target application." Also application specific context information may be conveyed in "URL data" and includes "context information comprising a session identifier and optionally a user or patient identifier" (Application page 10 lines 35-37). Support for encrypting an "address portion of said URL" and communicating "a single processed URL data string" including "said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form" is found between page 11 line 35 and page 13 line 24.

I. Rejection of claims 8 and 17 under 35 USC 112.

Claims 8 and 17 are rejected under 35 USC 112 second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter. Specifically, claims 8 and 17 are rejected as containing insufficient antecedent basis for the term "said corresponding authenticated different user identifier of said first application as said mapped user identifier" and "said corresponding authenticated different user identifier of said parent application as said mapped user identifier".

These terms have been amended to be "said authenticated different user identifier of said first application as a mapped user identifier" and "said authenticated different user identifier of said parent application as a mapped user identifier" in claims 8 and 17 respectively. As such these terms are compatible with the interpretation used in the Rejection and ensure antecedent basis is provided in the

respective base claims. Consequently this ground of rejection is no longer deemed to apply and its withdrawal is respectfully requested.

II. Rejection under 35 U.S.C. 102(e)

Claims 1, 3-8 and 10-23 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,178,511 – Cohen et al. These claims, as amended, are deemed to be patentable for the reasons given below.

Amended claim 1 recites a system "used by a first application for managing user access to at least one of a plurality of network compatible applications" comprising "an authentication processor for, receiving user identification information including a user identifier and initiating authentication of said user identification information using an authentication service; and at least one communication processor for, communicating an authentication service identifier and a corresponding user identifier to a managing application, said authentication service identifier identifying an authentication service used to authenticate identification information of said corresponding user and automatically communicating application specific context information in a data field of a URL to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information". These features are not shown or suggested in Cohen.

The system of amended claim 1 includes "automatically communicating **application specific context** information in a **data field of a URL** to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information". Such application specific context information includes a patient identifier or user identifier, for example (Application page 10 lines 35-37). The claimed system advantageously "automatically" communicates "**application specific context** information in a data field of a URL to a second application of said plurality of network compatible applications" such as a patient identifier "in response to authentication of said user identification information" initiated by the "authentication processor". Thereby the system enables a user to logon and authenticate with a first application such a patient census application and gain automatic access to multiple other applications such as a medical laboratory test result application and in response to user authentication with the test result application, be automatically provided with desired test results for the

specific patient selected in the first patient administration application (see example described on Application page 5 lines 8-12 and elsewhere in connection with Figure 2). This is done without the user having to re-enter context information (e.g., a patient identifier) by link selection or another command following automatic authentication with a second application. This capability is not shown or suggested in Cohen. The combination of automatic authentication to multiple applications together with automatic communication of application specific context information "in response to a user command to initiate execution of said second application and in response to authentication of said user identification information" facilitates user friendly operation and user seamless navigation in a plurality of concurrently operating applications. The system addresses the problems involved in "facilitating user initiation (e.g., logon), operation and termination (e.g., logoff) of multiple Internet applications and in securely passing URL, patient (and user) identification and other information between applications. A managing application is employed to coordinate user operation sessions. Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to **create a smooth user operation session**" (Application page 4 lines 23-31).

In contrast, Cohen does not mention, contemplate or suggest Internet based operation and communication of data via **URL** data fields. Cohen (alone or with any of the other references) also does NOT discuss or suggest "automatically" communicating "application specific **context** information in a data field of a URL" such as a patient identifier" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" initiated by the "authentication processor". Cohen discusses use of application specific information that supports user **logon**. Specifically, "for each of a set of users, a preferably global-accessible database (PKM) stores user-specific and application-specific information enabling the user to access and **logon** to one or more target resources" (Cohen abstract and column 2 line 62 to column 3 line 2). However, Cohen does not suggest **automatic** communication of "application specific **context**" information **after** logon and authentication to support **subsequent** seamless navigation. Cohen does not suggest Internet based operation and communication of "application specific context" data via **URL** data fields. Cohen also does not suggest these features in combination with facilitating automatic authentication to multiple network compatible applications" by "communicating an authentication service identifier" and a "corresponding user identifier to a **managing application**".

Consequently withdrawal of the Rejection of amended claim 1 under 35 USC 102(e) is respectfully requested.

Amended dependent claim 3 is considered to be patentable based on its dependence on claim 1. Claim 3 is also considered to be patentable because Cohen does not show or suggest a system in which "said communication processor also communicates a session identifier identifying a user initiated session of operation of said first application to said managing application and said user identification information includes a password associated with said user identifier". As recognized in the Rejection with respect to original claim 2, Cohen does not mention a "session identifier".

Dependent claim 4 is considered to be patentable based on its dependence on claim 1. Claim 4 is also considered to be patentable because Cohen does not show or suggest a system in which "said communication processor communicates said authentication service identifier and said corresponding user identifier to a managing application for **compilation** of a database". Contrary to the Rejection statement on page 3, Cohen in Column 4 line 64 to column 5 line 2 does not suggest "**compilation** of a database" including "authentication service identifier and said corresponding user identifier" data pairs. Cohen column 4 line 64 to column 5 line 2 recites "Preferably, PKM 24 is a secure, globally accessible repository that facilitates the single sign-on process. Although not meant to be limiting, with respect to a given user, the PKM (as will be described) preferably stores such information as a *username, a set of one or more password(s), and any other application environment-specific information such as domain name, hostname, application name, and the like.* Because this access information preferably is centralized in the PKM, users can access their target resources with one sign-on from any workstation. They can also manage their passwords from this one repository, as will also be seen". It is well understood that citation of a general list of items such as those italicized fail to provide 35 USC 112 compliant enabling disclosure of specific elements such as the recited "authentication service identifier and said corresponding user identifier" data pairs. Further, Cohen fails to show or suggest **communicating** "said authentication service identifier and said corresponding user identifier **to a managing application** for **compilation** of a database". In Cohen there is no suggestion of dynamic **"compilation"** of a database. There is no indication in Cohen of HOW the PKM repository is provided or any indication other than it is predefined.

Dependent claim 5 is considered to be patentable based on its dependence on claims 1 and 4. Claim 5 is also considered to be patentable because Cohen does not show or suggest a feature combination as in claim 5 involving a database "accessible by other applications of said plurality of network compatible applications for mapping a non-authenticated user identifier of a participant application to an authenticated and different user identifier of another application".

Amended independent claim 6 recites a "A system used for processing user access to network compatible applications" comprising "an authentication processor for, receiving authentication service identifier and corresponding user identifier data pairs from at least one of a plurality of applications, compiling a database using said data pairs, mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using said database; and at least one communication processor for, communicating said authenticated different user identifier to said second application and automatically communicating application specific context information in a data field of a URL to said second application in response to a user command to initiate execution of said second application".

Amended claim 6 is considered to be patentable for the reasons given in connection with claims 1, 4 and 5. Claim 6 is also considered to be patentable because Cohen does not show (or suggest) a feature combination as in claim 6 including "compiling a database" using "data pairs, mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using said database" and at least one communication processor for, "automatically communicating application specific context information in a data field of a URL to said second application in response to a user command to initiate execution of said second application". Cohen does not show or suggest "compilation of such a database" in combination with automatically communicating application specific context information in a data field of a URL to said second application in response to a user command to initiate execution of said second application". Cohen does not mention, contemplate or suggest Internet based operation and communication of data via URL data fields. Cohen (alone or with any of the other references) also does NOT discuss or suggest "automatically" communicating "application specific context information in a data field of a URL" such as a patient identifier" to a "second application" in "response to a user command to initiate execution of said second application". Cohen discusses use of application specific information that supports user logon and fails to contemplate or suggest automatic

communication of "application specific **context**" information **after** logon and authentication to support **subsequent** seamless navigation.

Dependent claim 7 is considered to be patentable based on its dependence on claim 6. Claim 7 is also considered to be patentable because Cohen does not show or suggest the feature combination of claim 7 in which "said authentication service identifier identifies an authentication service used to authenticate identification information comprising a user identifier of said corresponding user to provide an authenticated user identifier".

Dependent claim 8 is considered to be patentable based on its dependence on claim 6. Claim 8 is also considered to be patentable because Cohen does not show or suggest the feature combination of claim 8 in which "said authentication processor performs said mapping using said database by matching an authentication service identifier of said second application with an authentication service identifier of said first application and providing said authenticated different user identifier of said first application as a mapped user identifier".

Dependent claim 10 is considered to be patentable based on its dependence on claim 6.

Dependent claim 11 is considered to be patentable based on its dependence on claim 6. Claim 11 is also considered to be patentable because Cohen does not show or suggest the feature combination of claim 11 in which "said communication processor communicates a parameter to said second application, said parameter identifying success or failure of said mapping". The Rejection alleges this feature is shown in Cohen and relies for support on column 10 lines 35-37 ("Return codes from the interface are associated with buckets (rc_ success, rc_error, etc.), allowing the appropriate action to be taken based on the bucket into which the return code falls"). However, "Return codes... allowing the appropriate action to be taken based on the bucket into which the return code falls" does not show or suggest (or provide a 35 USC 112 enabling disclosure of) communicating "a parameter to said second application...identifying success or failure of" "mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using" a compiled "database". As previously explained Cohen does not discuss dynamic "compilation" of such a database at all.

Dependent claims 12 and 13 are considered to be patentable based on their dependence on claim 6.

Amended independent claim 14 recites a "system used for processing user access to Internet compatible applications" comprising "an authentication processor for, receiving an authentication service identifier and corresponding user identifier from a parent application, and mapping a non-authenticated user identifier of a child application to an authenticated different user identifier of said parent application; and at least one communication processor for, communicating said authenticated different user identifier to said child application and automatically communicating application specific context information in a data field of a URL to said child application in response to a user command to initiate execution of said child application and in response to communicating said authenticated different user identifier". Amended independent claim 14 is considered to be patentable for the reasons given in connection with claims 1, 4, 5 and 6.

Dependent claim 15 is considered to be patentable based on its dependence on claim 14. Claim 15 is also considered to be patentable because Cohen does not show or suggest the feature combination of claim 15 in which "said parent application establishes a session of user operation and said child application uses said authentication system to participate in said session of user operation". The Rejection relies on Cohen column 6 lines 38-45 in alleging this feature is shown in Cohen. The cited section just discusses logon and status information concerning logon. However, a "session" as known to one of ordinary skill in the art and as defined in the specification is a **user session of operation** and is **distinct** from, and different to mere logon. In the application, for example, "A parent application creates a session after the user is authenticated and before a child application is referenced. A parent application may delay establishing a session until a specific event, e.g., until the parent downloads (to a browser) a web page containing links to child applications" (Application page 6 lines 27-30). Therefore, a session is different from logon and is not suggested by logon. Cohen does not contemplate or discuss a "session" at all. Consequently, Cohen does NOT show or suggest a system in which a "parent application establishes a session of user operation and said child application uses said authentication system to participate in said session of user operation".

Dependent claims 16-20 are considered to be patentable based on their dependence on claim 14 and any intervening claim and because of the additional

feature combinations they represent for the reasons given in connection with previous claims.

Amended independent method claim 21 mirrors apparatus claim 14 and is considered to be patentable for similar reasons.

Dependent claim 22 is considered to be patentable based on its dependence on claim 21 for reasons given in connection with claim 6.

Amended independent method claim 23 mirrors apparatus claim 1 and is considered to be patentable for similar reasons. Consequently withdrawal of the Rejection of claims 1, 3-8 and 10-23 under 35 USC 102(e) is respectfully requested.

III. Rejection under 35 U.S.C. 103(a)

Claims 2 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,178,511 – Cohen et al in view of U.S. Patent 5,884,312 – Dustan et al.. These claims, as amended, are considered patentable for reasons given in connection with claim 1 and for the following reasons.

Amended dependent claim 2 recites a system in which "said application specific context information comprises at least one of, (a) a user identifier and (b) a patient identifier and said communication processor encrypts said address portion of said URL and incorporates, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string". These features are not shown or suggested in Cohen with Dustan.

Amended dependent claim 2 is considered to be patentable based on its dependence on claim 1. Neither Cohen nor Dustan mention, contemplate or suggest Internet based operation and communication of data via URL data fields. Cohen with Dustan also does NOT discuss or suggest "automatically" communicating "application specific context information in a data field of a URL" such as a patient identifier" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" initiated by the "authentication processor". Cohen discusses use of application specific information that supports user logon. Specifically, "for each of a set of users, a preferably global-accessible database (PKM) stores user-specific and application-

specific information enabling the user to access and **logon** to one or more target resources" (Cohen abstract and column 2 line 62 to column 3 line 2). However, Cohen with Dustan does not suggest **automatic** communication of "application specific **context**" information **after** logon and authentication to support **subsequent** seamless navigation. Cohen with Dustan does not suggest Internet based operation and communication of "application specific context" data via **URL** data fields. Cohen also does not suggest these features in combination with facilitating automatic authentication to multiple network compatible applications" by "communicating an authentication service identifier" and a "corresponding user identifier to a **managing application**".

Further, Cohen with Dustan fails to suggest a system that "encrypts said address portion of said URL and incorporates, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string". These features address the security deficiencies of URL processing functions of electronic systems. "Applications are vulnerable to the corruption of URL data and the context information conveyed within the URL data. The URL data conveyed from application 200 to application 230 includes context information comprising a session identifier and optionally a user or patient identifier. This URL data is potentially vulnerable to corruption to cause URL replay or redirection of an application to a substitute address or to gain access to application functions and parameters for unauthorized purposes. In order to protect against such corruption and to ensure that the entity being accessed is the one originally targeted, portions of the URL data conveyed between applications are advantageously encrypted" (Application page 10 line 36 to page 11 line 7).

The claimed system addresses the security problem by ensuring "that a URL link (e.g. a URL link to child application 230) embedded in a web page provided for display using browser 10 is not redirected. For this purpose, application 200 generates a hash value from the domain, path, program, and program data portion of the URL. Application 200 (as the sending application) generates a hash value from the fully qualified URL link" (Application page 9 lines 30-34). "Application 230 decrypts the received hash value for comparison with a corresponding hash value independently generated from corresponding URL data retrieved from a web server". Specifically, the "independently generated hash value and the hash value received by application 230 from application 200 via browser 10 are compared and if they are not equal, the request to initiate application 230 is rejected" (Application page 10 lines 23-35).

Cohen with Dustan fails to suggest a system that "encrypts said address portion of said URL and incorporates, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string". Consequently withdrawal of the Rejection of amended claim 2 under 35 USC 103(a) is respectfully requested.

Amended dependent claim 9 is considered to be patentable based on its dependence on claim 6. Claim 9 is also considered to be patentable because of reasons given in connection with claim 2.

Consequently withdrawal of the Rejection of claims 1-23 is respectfully requested.

In view of the above amendments and remarks, Applicants submit that the Application is in condition for allowance, and favorable reconsideration is requested.

Respectfully submitted,

Date: 13 January 2005

Alexander J. Burke
Reg. No. 40,425

SIEMENS CORPORATION
CUSTOMER NO. 28524